Name :- Nikhil Kumar Roll no :- 1806055
Branch :- CSE-1 program code :- UG-CS
Course Title :- Information security.
Course code :- CS6404 Exam date :- 22/05/21

Q(1) The Roll no of mine = 1806055
Ans :- last 3 digit in my roll no :- 055
So, that message that to be ~~encrypted~~ encrypted in SS in RSA Algorithm.

p = 19
Q = 13
e = 11
r = (p-1)(q-1)
N = pq = 13 × 13
= 247
r = (19-1)(13-1)
= 18 × 12
= 216
Now we need to find the private key d such that
e * d = 1 mod r
11 * d = 1 mod 216
11 * d mod 216 = 1 (By using extended eccliden algorithm)

So that 11 & 216 are relatively prime and d & 216 are relatively prime.

k = 11 * d
⇒ k mod 216 = 1
So k = 649 which is multiple of 11
k = 649

Name:- Nikhil Kumar Roll no:- 1806055
Branch:- CSE-I Program code:- UG_CS
Course Title:- Information Security
Course code:- CS6404 Exam date:- 22/05/21

$\Rightarrow 11 \times 59 = 1 \times d$

$d = 59$

So private key $(d) = 59$

Now we need to encrypt the secret message such that

cipher $= (msg)^e \bmod N$

$\Rightarrow msg = 97$ (my roll no: 1806055)

Cipher $= (55)^{11} \bmod 247$

$= 167$

we can check our answer by decrypting the cipher using the private key (d) by

$msg = (cipher)^d \bmod N = (167)^{59} \bmod 247 = 55$

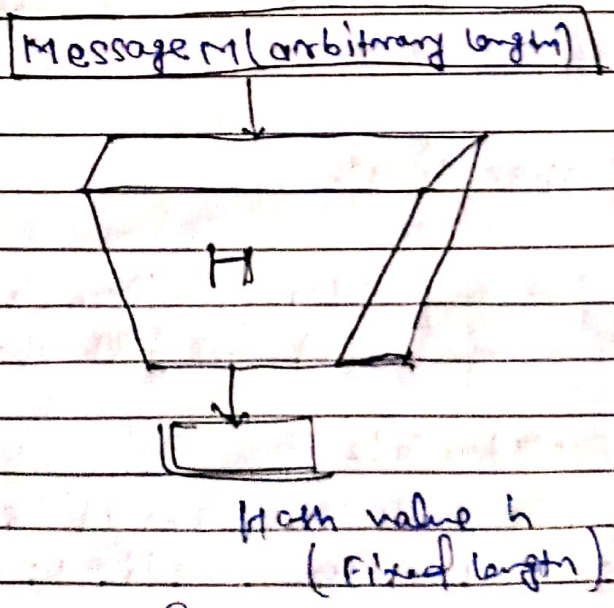
∴ The cipher text for 55 is 167

Name :- Nikhil kumar Roll no :- 1806055
Branch :- CSE 1 Program code :- VH-CS
Course Title :- Information Security.
Course code :- CS6404 Exam date :- 22/05/21

Q(2)

Ans :- **Properties of a HASH function :-**

- H(x) is easy to compute for any given x.
- For any given block x, it is computationally infeasible to find x such that H(x) = h (deterministic)
- The hash value is fully determined by the data being hashed.
- The hash function "uniformly" distributes the data across the entire set of possible hash value.
- A small change to a message should change the hash value so extensively that the new hash value appears uncorrelated with the old hash value



Name :- Nikhil kumar Roll no :- 180655
Branch :- CSE 1 Programcode :- UN_CS
Course Title :- Information security
Course code :- CS6404 Exam date :- 22/05/21

Hash functions are extremely useful and appear in almost all information security applications

A hash function is mathematical function that converts a numerical input value in to another compressed numerical input value the input to the hash function is of arbitrary length but output is always of fixed length.

- Fixed length output (Hash value) :
- Hash function converts data of arbitrary length to a fixed length. this process is often referred to of hashing the data.

- Hash function with n bit output is referred to as an n-bit hash function. popular hash function generate values ~~of~~ b/w 160 and 512 bit.

- Efficiency of operation :-

- Generally for any hash function h with input x computation of h(x) is fast operation.

- pre-Image Resistance :-

this property means that it should be computationally hard to reverse a hash function.

Name:- Nikhil kumar Rollno:- 1806055
Branch:- CSE-1 programcode:- UN-CS
Course Title:- Information security
Course code:- CS6404 Exam Date:- 22/05/21

Q (2) cryptographic hash function:-

Ans ⇒

→ it is a mathematical algorithm that maps data arbitrary size to a bit array fixed size

→ it is a one-way function that is a function which is practically infeasible to invert

Q (3) Df

- Different on avalanche effect:- A change in just one bit the original password is changed the output of enciphered text should change, it is unpredictably and unpredictably.
- Deterministic:- for a given block x, it is computationally infeasible to find x such that $H(x)=h$.
- collision resistant:- H should be hard to find two different password that hash to the same enciphered text.

Name:- Nikhil kumar Roll no:- 1806055
Branch:- CSE I Program code:- UH-CS
Course Title:- Information security.
Course code:- CS6404 Exam date:- 22/05/21

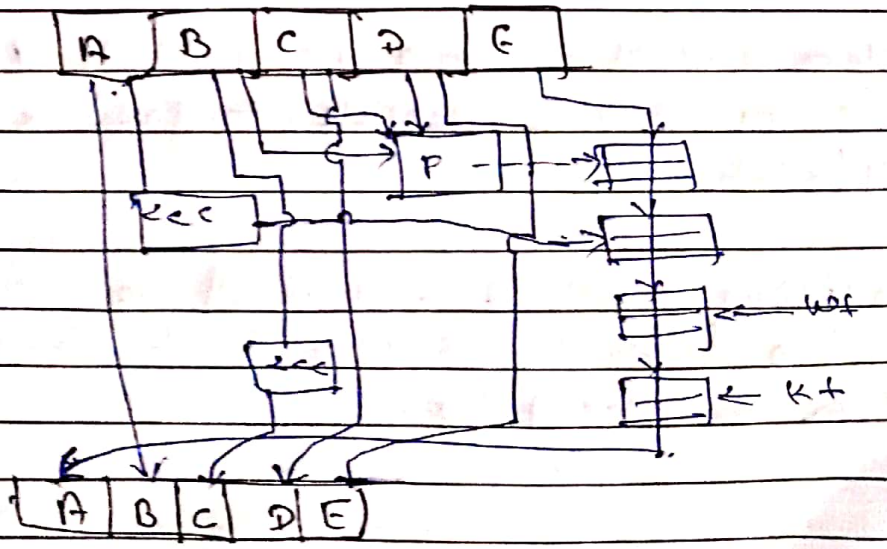
2.

SHA1 Ans:-

→ It takes an input and produce a 160-bit (20-byte) hash value known as message-digest

→ Function:-
(A, B, C, D, and E) → 32-bit words of the state

(a) f is a non-linear function that varies.
(b) left shift n (n varies), denote left bit rotation by n place.
(c) Wt is the expanded message word of round t
(d) Kt is round constant at round t
(e) Red sequence denotes addition modulo 2^{32}



Name :- Nikhil Kumar Roll no :- 1806058
Branch :- CSE-1 program code :- UH-CS
Course Title :- Information security
Course code :- CS6404 Exam date :- 22/05/21

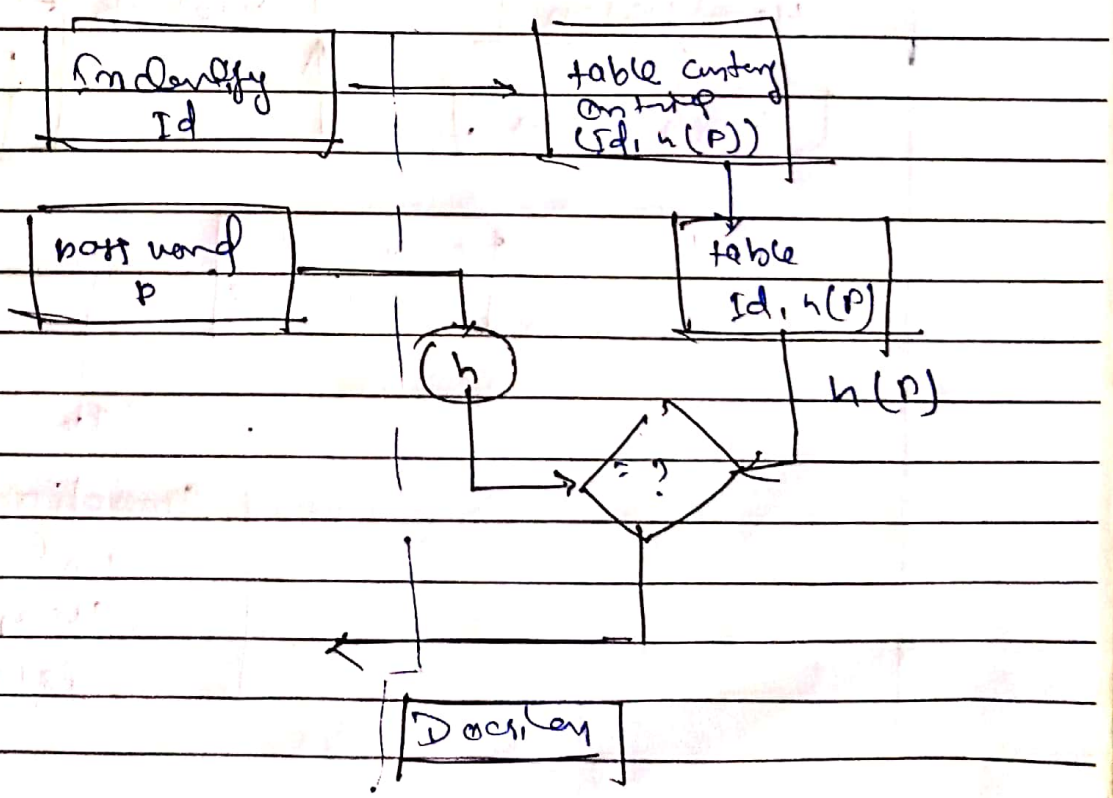
The cryptography use of hash function are :-

(i) password storing :-

→ Hash function provide protection to password storage instead of storing password, the hash value of password is stored on the file.

→ password file consists of table of pwd as the form of (user id, h(p))

→ process of login is as follows :-



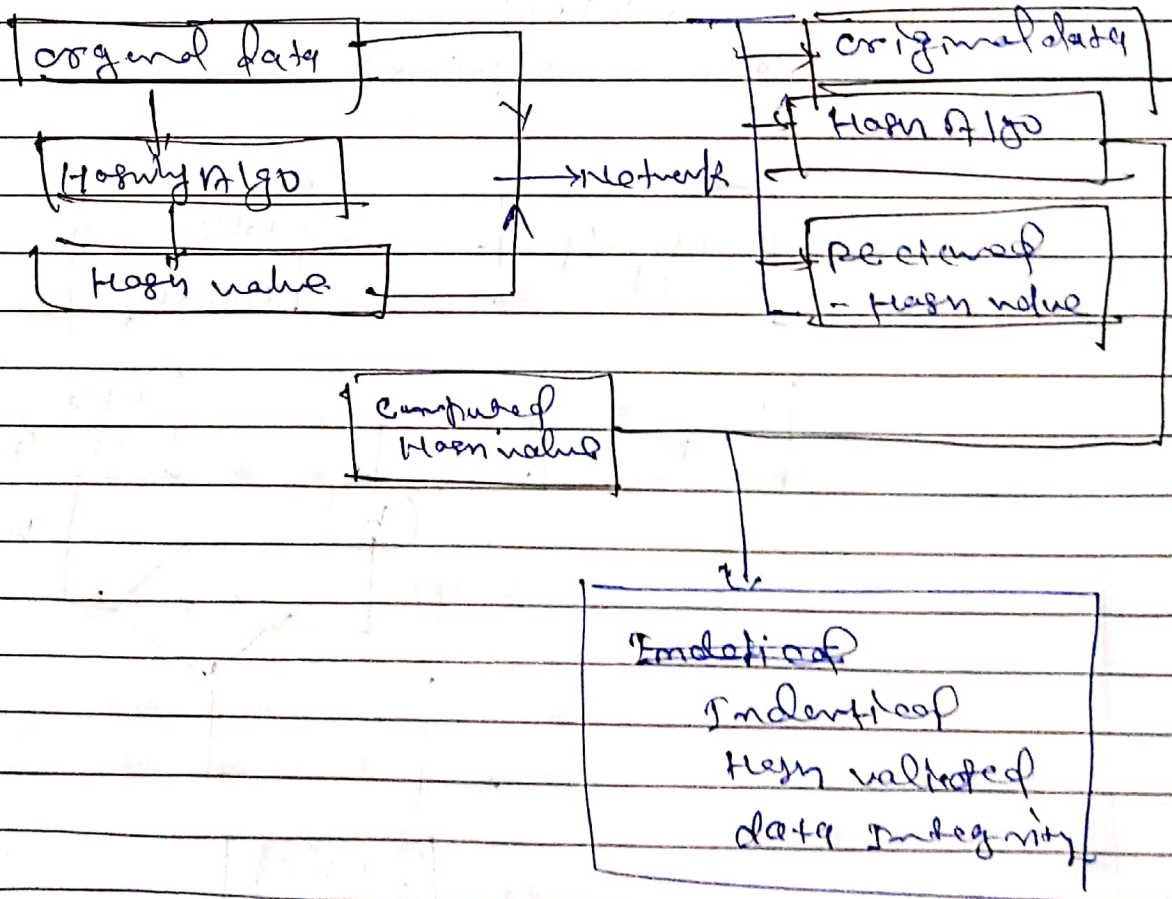
→ An only see the hash of password. but we can not we intend to login the system.

Q 11

Name :- Nikhil Kumar | Roll no :- 1806055
Branch :- CSE-1 | program code :- UH-CS
Course Title :- Information security
Course code :- CS6404 | Exam date :- 22/05/21

(ii) Data integrity check

It is a common application of hash function. It is used to generate checksum on data files that provides assurance about a data's identity check.



Name:- Nikhil kumar Roll no:- 180655
Branch:- CSE 1 Program code:- UG-CS
Course Title:- Information Security.
Course code:- CS6404 Exam date:- 22/05/21

Q(3) (i) Ans:-

Authentication versus access control:-

Ans:- To protect content from unauthorized application user, and to control access to administrative functions, web-based content Analytics supports user authentication and authorization (access controls).

Authorization (access control):-

Authorization is any mechanism by which a system grants or revokes the right to access some data or perform some action. often, a user must log in to a system by using some form of authentication. Access control mechanisms determine whether a user can or cannot do by comparing the user's identity to an access control list (ACL).

Different types of authenticating users:-

5 common Authentication Types:

(i) password-based authentication:-

Passwords are the most common methods of authentication. password can be in the form of a string of letters, numbers or special characters. To protect yourself you need to create a strong password that include a combination of all possible options.

Name :- Nikhil kumar Roll no :- 1806055
Branch :- CSE-1 Programme code :- UH-CS
Course Title :- information security.
Course code :- CS6404 Exam date :- 22/05/21

(2) Multi-factor authentication :-

→ multi-factor Authentication (MFA) is an authentication methods that requires two or more independent ways to identify a user. Example :- smart phone, captcha test, fingerprint, or facial recognition.

(3) certificate-based authentication :-

→ certificate-based authentication technology identify user, machines or devices by using digital.

(4) Biometric authentication :-

→ Biometric authentication is a security process that relies on the unique biological characteristics of an individual. there are key advantages of using biometric authentication technology.

(5) Token-based authentication :-

→ Token-based authentication technology enable user to enter their credentials once and receive a unique encrypted string of random character in exchange.

Name:- Nikhil kumar Roll no:- 1806055
Branch:- CSE-I Program code:- UH-C8
Course Title:- Information security.
Course code:- CS6404 Exam Date:- 22/03/21

Types of information security policy:-

There main types of policies exist:-

1. organizational (or master) policy.
2. System-specific policy
3. issue-specific policy.

→ organizational policy:- it is the strategic plan for implementing security in the organization.

→ System-specific policy:- it concerned with a specific individual computer system. It is meant to prepare the approved software, hardware and hardening methods for that specific system.

→ issue-specific policy:- it concerned with certain specific areas that may require more attention. for this reason.

Examples of this types of policy:-
→ change management policy.
→ physical security policy.
→ Email policy.
→ Encryption policy
→ vulnerability management policy
→ Data retention policy
→ Access control policy.

Name:- Nikhil kumar Rollno:- 1806055
Branch:- CSE-1 Program code:- UH-CS
Course Title:- Information Security.
Course code:- CS6404 Exam Date:- 22/05/21

* Guideline:-

→ A guideline point to a statement in a ~~poli~~ policy or procedure by which to determine a course of action. It are commendation or suggestion of how things should be done.

→ Baseline:-

→ A A baseline is a minimum level of security that a system network or device must adhere to. Baseline are usually mapped to industry standards.

Procedures:-

→ A procedure is the most specific of security documents. A procedure is a detailed, in-depth step-by-step document that details exactly what is to be done. As an analogy,

Name :- Nikhil kumar
Roll no :- 180055
Branch :- CSE-I
Program code :- UN_CS
Course Title :- Information security
Course code :- CS6404
Exam date :- 22/05/21

Q(4)
Ans :-

My Roll Number = 180055

key, k = 1111

plaintext = 1011 1010 0011 1111

Steps of algorithm

C = NULL

N = 16/8 = 2

m = b1, b2 b1 = 10111010
b2 = 00111111

for block b1

for j = 1

b1 = L1 and R1

L1 = 1011 , R1 = 1010

R1 = R1 ⊕ K

1010 ⊕ 111 = 0101 R1 = 0101

1010 ⊕ 1011 = 001

R1 = (0101) = 1010

R1 = R1 ⊕ L1

Name :- Nikhil Kumar Roll no :- 1806055
Branch :- CSE II Program code :- UG-CS
Course Title :- Information Security.
Course code :- CS6404 Exam Date :- 22/04/21

$$\begin{array}{r} 1010 \\ \oplus\ 1011 \\ \hline 0001 \end{array}$$

$j \neq 2$, so it is ignored

for $j = 2$, 2 rounds

$b_1 - L_2$ and R_2
1110 0001

$R_2 = R_2 \oplus K$ 0001

$$\begin{array}{r} \oplus\ 1111 \\ \hline 1110 \end{array} \quad R_2 = 1110$$

$R_2 = \overline{R_1} = 0001$

$R_2 = R_2 \oplus L_2$ 0001

$$\begin{array}{r} \oplus\ 1110 \\ \hline 1111 \end{array}$$

$i = 2$ $C_2 = L_2 R_2 = 11101111$

$L_3 = R_2 = 1111$

$R_3 = L_2 = 1110$

$K = K << 2$ $K = 1111$

final ciphertext $C = C_1 C_2$

$= 00011010111111 0$

Name :- Nikhil Kumar Roll no :- 180605
Branch :- CSE-1 Program code :- UG_CS
Course Title :- Information Security.
Course code :- CS6404 Exam date :- 22/05/21

$C = C + C_1 = 00011010$

for block b_1,

for $j = 1$

b_2 = in L_1 and R_1 $b_2 = 00111111$

$L_1 = 0001$, $R_1 = 1111$

$R_1 = R_1 \oplus K$ 1111
$\oplus$1111 $R_1 = 0000$
0000

$R_1 = R_1 = 1111$

$R_1 = R_1 \oplus L_1$ 1111
$\oplus$0001 $R_1 = 1110$
1110

if $i \neq 2$ 80 if is ignored

$L_2 = R_1 \Rightarrow L_2 = 1110$
$R_2 = L_1 \Rightarrow R_2 = 0001$

$K = K << 2 \Rightarrow K = 1111$

$C_1 = L_2 R_2 = 11100001$

Name :- Nilkhil Kumar Roll no :- 1806055
Branch :- CSE 1 program code :- UH-CS
Course Title :- Information security.
Course code :- CS6404 Exam Date :- 22/05/21

$L_2 = R_1 \Rightarrow L_2 = 0001$

$R_2 = L_1 \Rightarrow R_2 = 1011$

$K = K << 2$

$= (1111) << 2 = 1111$

$C_1 = L_2 R_2$

$= 0001 1011$

for $j = 2$

$b_1 = L_2$ and R_2

$= 0001, 1011$

$R_2 = R_2 \oplus K$ 1011
+1111
0100 $R_2 = 0100$

$R_2 = \overline{R_2} = 1011$

$j == 2$, so enter in if

$C_1 = L_1 R_1$

$= 00011010$

$L_3 = R_2 = 1011$

$R_3 = L_3 = 0001$

$K = 1111$